METHOD AND APPARATUS FOR SAFELY DECIDING VARIOUS STATES OF HISTORY OF COMMODITY

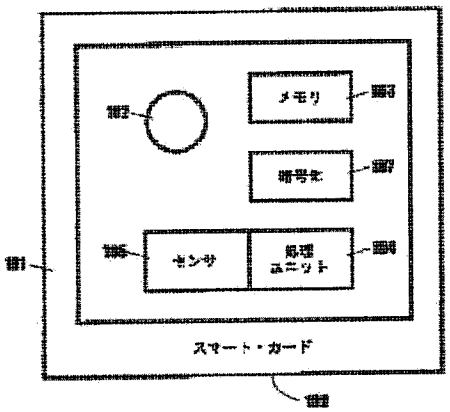
Publication number: JP2000205892 (A)
Publication date: 2000-07-28
Inventor(s): TIMOTHY J CHEINAA; GREENGARD CLAUDE A; WILLIAM R PUURIIBURANKU; CHARLES P TORESE; CHAI W WOO +
Applicant(s): IBM +
Classification:
- international: ***G01D1/00; G06F21/06; G06K19/00; G06K19/07; G06K19/073; G06K19/10; G06Q10/00; G06Q50/00; G07F9/02; G07G1/00;*** **G01D1/00; G06F21/00; G06K19/00; G06K19/07; G06K19/073; G06K19/10; G06Q10/00; G06Q50/00; G07F9/02; G07G1/00;** (IPC1-7): G01D1/00; G06F17/60
- European: G06K19/073; G06K19/073A8; G06K19/073A8A; G06K19/07T; G07F9/02; G07G1/00C2D
Application number: JP20000000897 20000106
Priority number(s): US19990228231 19990111

Also published as:
JP3703075 (B2)
EP1020813 (A2)
EP1020813 (A3)
US2002186145 (A1)
US6501390 (B1)

more >>

Abstract of **JP 2000205892 (A)**

PROBLEM TO BE SOLVED: To provide accurate information of a product to resist an effort for concealing a symptom such as tampering (illegal tearing) or the like, by sensing data regarding a state of an environment of an object (product) by a sensor, encoding a signal from the sensor and recording the signal. SOLUTION: A smart card 101 mounted on a product is energized by a small power source such as a battery 102 or the like. In addition to constituents such as a memory 103, a processing unit 104, an encoding module 107 and the like, a sensor 105 for detecting a change of the product or an environment caused by tampering is provided. In the module 107, an encryptional algorithm such as, for example, Menezes, Oorschot or the like is used. The overall card 101 can be protected by a tamper-proof package 109.; Recording data is encoded to provide a history of a physical event of the product. A person having a key can take out data by anyone, and can decide the state of the product.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－205892
（P2000－205892A）
(43)公開日　平成12年７月28日(2000.7.28)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０１Ｄ　1/00		Ｇ０１Ｄ　1/00	C	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Z	

審査請求　有　　請求項の数23　ＯＬ　（全 8 頁）

(21)出願番号　特願2000－897(P2000－897)

(22)出願日　平成12年１月６日(2000.1.6)

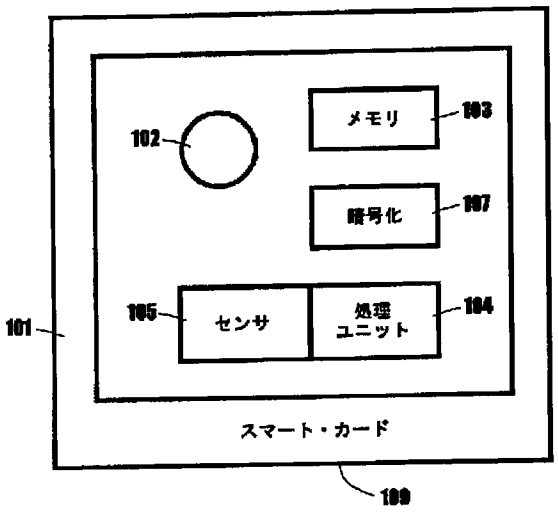
(31)優先権主張番号　０９／２２８２３１
(32)優先日　平成11年１月11日(1999.1.11)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　ティモシー・ジェイ・チェイナー
アメリカ合衆国　ニューヨーク州マホパック　パレット・ヒル・ロード　161
(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　商品の履歴の諸態様を安全に判定するための方法および装置

(57)【要約】
【課題】　本発明は、１）製品の使用、２）取り扱い、３）タンパリング、４）製品の環境（極端な温度、湿度または衝撃などの環境の変化が製品の劣化をもたらす可能性があるので）のうちの１つまたは複数に起因する影響を含む製品の物理的履歴を検出し、信頼性のある形で記録する方法および装置を提供する。
【解決手段】　この装置には、１つまたは複数のセンサと組み合わされ、製品または環境に対する外部の影響を記録し、これらの変化を暗号化された形で記録する、「スマート・カード」またはより一般的には「スマート・トークン」が含まれる。この情報は、（おそらくは公開）復号鍵を有する人物であれば誰でも検証できるが、この情報を変更する能力は、応用分野に応じて、暗号化鍵へのアクセス権を有する人物に制限される。さらに、この装置には、特にその装置が取り付けられると思われる製品に装置が取り付けられていることを確認するために、信頼性のある形で検証できる認証情報が含まれる。



【特許請求の範囲】
【請求項１】オブジェクトまたは前記オブジェクトの環境の状態に関するデータを、複数のセンサのうちの少なくとも１つを用いて感知するステップと、
前記センサからの信号をスマート・タグ内に組み込まれた記憶装置へ安全に送るステップと、
後の取出のために前記記憶装置内で前記信号の暗号化を使用して安全に記録するステップとを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも１つに関する集積スマート・タグ内の情報を安全に記録し、記憶する方法。
【請求項２】さらに、前記記憶装置内に記録された前記信号のそれぞれについて、前記記憶装置内で時刻を記録するステップを含む、請求項１に記載の方法。
【請求項３】前記センサが、温度、湿度、圧力、光、振動、衝撃、電磁界および化学組成を含むグループから選択された、前記オブジェクトの１つまたは複数の状態の変化を検出する、請求項１に記載の方法。
【請求項４】前記オブジェクトが、自動車であり、前記センサが、時刻、総マイル数、衝撃、温度、地理的位置、速度を含むグループのうちの少なくとも１つを検出し、前記記憶装置内で前記信号の暗号化を使用して安全に記録し、前記自動車の時間シーケンス履歴を作成する、請求項１に記載の方法。
【請求項５】前記オブジェクトが、薬理学製品、食品または化学製品を納めるパッケージング・コンテナであり、前記センサが、温度、湿度、圧力、光、振動、衝撃、電磁界、化学組成および前記パッケージング・コンテナの開封のグループのうちの少なくとも１つを検出する、請求項１に記載の方法。
【請求項６】前記オブジェクトが、電子消費者製品であり、前記センサが、前記消費者製品の電源投入時間の数を検出する、請求項１に記載の方法。
【請求項７】オブジェクトまたは前記オブジェクトの環境の状態に関するデータを、複数のセンサのうちの少なくとも１つを用いて感知するステップと、
前記データの複数の関数のうちの少なくとも１つを計算するために前記データを処理するステップと、
前記データと前記関数の値との組み合わせを記憶装置に記憶するステップとを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも１つに関する集積スマート・タグ内の情報を記録し、記憶する方法。
【請求項８】さらに、前記記憶装置での記憶の前に、前記データおよび前記関数の前記値のうちの少なくとも１つを暗号化するステップを含む、請求項７に記載の集積スマート・タグに情報を記録し、記憶する方法。
【請求項９】さらに、前記処理ステップからの結果を表示するステップを含む、請求項７に記載の集積スマート・タグに情報を記録し、記憶する方法。
【請求項１０】記憶装置と、
前記記憶装置に信号を安全に送るセンサと、
後の取出のために前記記憶装置に安全に記録された前記信号からのデータを変更する暗号化モジュールとを含む、スマート・タグ・セキュリティ・システム。
【請求項１１】さらに、前記センサからの前記信号に作用する処理ユニットを含む、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項１２】前記信号が前記記憶装置への記録に関する閾値を満たすかどうかを判定するために、前記処理ユニットが前記信号に作用する、請求項１１に記載のスマート・タグ・セキュリティ・システム。
【請求項１３】オブジェクトの状態を判定するために前記信号を処理するためのアルゴリズムを実行するために、前記処理ユニットが前記信号に作用する、請求項１１に記載のスマート・タグ・セキュリティ・システム。
【請求項１４】さらに、前記処理ユニットによって判定された結果を表示する表示装置を含む、請求項１１に記載のスマート・タグ・セキュリティ・システム。
【請求項１５】前記表示装置に、安全なアクセスが含まれる、請求項１４に記載のスマート・タグ・セキュリティ・システム。
【請求項１６】前記スマート・タグが、単一のシリコン基板に集積される、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項１７】さらに、前記センサから記録される信号のそれぞれについて、記録されるタイム・スタンプを前記記憶装置に送るタイミング・ユニットを含む、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項１８】前記センサが、前記センサの周囲の圧力の変化に応答して前記記憶装置に信号を送る圧力センサからなる、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項１９】前記センサが、前記センサへの露光量が変化した時に前記記憶装置に信号を送る光センサからなる、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項２０】前記センサが、破壊された場合に前記記憶装置に信号を送る電気接続からなる、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項２１】さらに、前記セキュリティ・システムによって保護されるオブジェクトに固有の、前記記憶装置内で暗号化された識別コードを含む、請求項１０に記載のスマート・タグ・セキュリティ・システム。
【請求項２２】前記識別コードが、ゼロ知識プロトコルを使用して認証される、請求項２１に記載のスマート・タグ・セキュリティ・システム。
【請求項２３】オブジェクトまたは前記オブジェクトの環境の状態に関するデータを感知するためのセンサと、

前記データの複数の関数のうちの１つを計算するためのプロセッサと、
記憶装置に前記データと前記データの前記関数の値とを記憶するための記憶装置とを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも１つに関する集積スマート・タグ内の情報を記録し、記憶するためのスマート・タグ・セキュリティ・システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、全般的には消費財のセキュリティに関し、具体的には、製品セキュリティの維持におけるスマート・タグの使用に関する。
【０００２】
【従来の技術】潜在的な消費者に所有される前に、製品または商品がこうむった事象の結果としての製品の現在の状態に関する情報を提供することのできる装置を備えた製品の必要がある。その例には、消費者によって使用される前の医薬品または食品の状態が含まれる。
【０００３】また、消費者は、時々、製品が新品であるか否かを知る権利または必要を有する。これは、高価な品目の場合に特にそうである。また、製品の履歴のいくつかの態様、たとえば自動車の場合では非常に安全ではないが現在オドメータに示される、自動車の履歴の１態様を、記録することのできる装置を製品が備えることも必要である。
【０００４】本発明のためのもう１つの文脈は、いくつかの場合に、ある製品のコンテナが、製造業者によって再利用され、消費者が、コンテナ内の製品が新しいか否かと、許可されていない第三者によってそのコンテナが再利用されたかどうかを知りたいと思うという事実である。また、欠陥のため、有効期限を過ぎたため、または、たとえば過度の冷却、加熱、湿度などの形の環境の望ましくない変化のためのいずれかで、製品が劣化したかどうかを検出する方法が必要である。これらのシナリオでは、使用、取り扱い、タンパリング（不正開封）または環境要因の結果として製品が受けた物理的な力を検出できる装置が必要である。人間の介入または環境要因のいずれかについて、いくつかの情況では、そのような事象の記録された履歴の変更または偽造が非常に困難であることが重要な場合がある。
【０００５】従来技術には、パッケージがタンパリングされた時を検出できるようにする、封印と封入を用いる多数の方法が含まれる。このような従来技術は、歴史上はるかにさかのぼり、技術の全般的な進歩から利益を得る、非常に一般的または非常に具体的な使用に関する多数の改良が提案されてきた。たとえば、米国特許第５１５９６２９号明細書には、電子アセンブリをタンパリングから保護するための侵入バリアが記載されている。従来技術には、米国特許第５０１０５６０号明細書に記載のように、製品に対する情報を記憶するデータ・ロガーなどの年代順の情報を記録する方法も含まれる。
【０００６】しかし、これらの方法は、製品またはその環境もしくはこの両方のタンパ・エビデント（tamper evident、タンパリングがすぐにわかる）履歴（ヒストリー）を提供するという問題を克服しない。従来技術を用いると、製品またはその環境もしくはこの両方の履歴に関する情報を安全に記録し、保持することができない。
【０００７】
【発明が解決しようとする課題】したがって、本発明の目的は、製品がタンパリングを受けた時を検出し、タンパリングを行う者または、タンパリングを隠すことから利益を得る者か、タンパリングの徴候を隠すための労力に抵抗することができる、従来技術のタンパ・エビデントなパッケージングに対する新規の改良を提供する。
【０００８】
【課題を解決するための手段】以下では、「変更が不可能」や「タンパ・プルーフ（tamper-proof）」などの用語は、攻撃に耐えるために十分な資源が持ち込まれる場合にコードなどが理論的に破壊される可能性があるので、コスト／利益の問題に起因して成功裡の攻撃がまれになるようにするために、タンパリングに対する十分な抵抗が提供される状況を記述するものとして理解されたい。
【０００９】本発明は、米国特許第３９７１９１６号明細書、米国特許第４００７３５５号明細書、米国特許第４０９２５２４号明細書および米国特許第４１０２４９３号明細書に記載のスマート・カード、または、より一般的にはスマート・トークンを、製品またはスマート・カードもしくはその両方に取り付けられたセンサと組み合わせて使用する。タンパリングの際または他の状況に対する応答として、センサは、暗号化され、製品に取り付けられたスマート・カードのメモリまたは記憶装置に記憶される信号を生成する。
【００１０】たとえば、ゼロ知識プロトコルを使用することによって、スマート・カードを認証することはできるが、複製することはできないことを想起されたい。この技術は、たとえば米国特許第５１４０６３４号明細書に開示されている。これは、スマート・カードの特徴を表す特性である。したがって、この開示の残りでは、これらの特性を有し、なんらかのメモリまたは処理能力もしくはその両方を有する電子構成要素を、実際にカードに類似した形態をとらない場合であっても「スマート・トークン」または「スマート・カード」と呼称する。スマート・カードの技術および応用分野に関する一般的な参考資料は、ドレイファス（Henry Dreifus）およびモンク（J. Thomas Monk）共著「Smart Cards: A Guide to Building and Managing Smart Card Applications」、John Wiley &; Sons刊、１９９８年にある。
【００１１】製品またはそのパッケージングがタンパリ

ングされる時には、製品またはその環境の何らかの属性が変化する。この変化は、スマート・カードに取り付けられたセンサによって（少なくともそのうちの一部で）検出されるものであり、スマート・カードは、スマート・カード・メモリ内に、消去または何らかの情報の書込によって、この変化を不可逆的に記録する。スマート・カードは、ゼロ知識プロトコルを使用することによって、複製に抵抗するようにもされており、その結果、元の製品の製造業者または、たとえばおそらくは信頼される第三者だけが、そのようなスマート・カードを製造または購入することができる。スマート・カードは、その内部メモリにこれらの変化の履歴を記録することもできる。

【００１２】

【発明の実施の形態】ここで図面、具体的には図１を参照すると、製品１０６に取り付けられたスマート・カード１０１が示されている。図２に示されているように、スマート・カードは、電池１０２などの小さい電源によって給電される。メモリ（または記憶装置）１０３、処理ユニット１０４、暗号化モジュール１０７などの、スマートカード内の通常の構成要素のほかに、このスマート・カードは、タンパリングに起因する製品または環境の変化を検出することのできるセンサ１０５（または複数のセンサ）にも接続される。

【００１３】暗号化モジュールでは、たとえばメネゼス（Alfred J. Menezes）、オールショット（Paul C. van Oorschot）およびバンストーン（Scott A. Vanstone）共著、「Handbook of Applied Cryptography」、CRC Press刊、１９９７年に記載の、Rivest, Shamir and Adleman (RSA) または暗号化基準 (DES) などの周知の（公開鍵または秘密鍵）暗号化アルゴリズムのいずれかを使用することができる。スマート・カードに関連する暗号化問題に関する議論は、前述のドレイファスおよびモンクの書籍にある。暗号化アルゴリズムは、スマート・カードのメイン・プロセッサ上でソフトウェア・モジュールとして実施することができ、専用ハードウェアで実行することもできる。パーソナル・コンピュータに対する暗号アクセラレータとして現在使用されているそのような専用ハードウェアの１例が、カナダ、オンタリオ州のChrysalis-ITS社が製造するＬｕｎａＶＰＮ暗号アクセラレータである。

【００１４】スマート・カード全体を、米国特許第５１５９６２９号明細書に記載のものなどのタンパ・プルーフ・パッケージ１０９によって保護することができる。スマート・カードは、スマート・カード内のデータを判定または変更しようとする試みのすべてが、スマート・カードのこのデータの消去またはある要素の破壊をもたらすという意味で、タンパ・エビデントでなければならない。スマート・カード自体に対するタンパリングを防ぐために、パッケージングに、センサとの閉じた接続を形成するトリップ・ワイヤまたは磁気回路を含めることができ、製品に対するタンパリングには、この接続を破壊し、スマート・カード内の（不可逆）変化のトリガになる形でパッケージングを開くことが伴う。いくつかの情況では、タンパ・プルーフ機能と暗号化が必要でない場合がある。

【００１５】スマート・カードまたはそのデータ内容の変更または複製を防ぐという同一の目的に他の機構を使用することもでき、その例には、米国特許第５１５９６２９号明細書の発明の簡単な変更として得られる。

【００１６】センサは、オンチップ圧力センサか、米国カリフォルニア州FremontのLucas NovaSensor社が製造するＮＰＰ、ＮＰＣまたはＮＰＨシリーズ圧力センサなどの圧力センサとすることもでき、製品は低圧でパッケージングされる。製品のタンパリングでは、パッケージングを開き、外部の圧力がこのセンサに達することができるようにする必要がある。この圧力変化が、スマート・カードによって記録される。保護を改良するために、パッケージに、パッケージ内部の圧力をランダムに変化させるポンプを含めることもできる。この場合、圧力センサは、パッケージ内部の圧力P_{sensor}を測定し、センサの読みとポンプへのプロセッサ・コマンド$P_{computer}$を比較する。差分信号は、次式によって計算される

【数１】

$$P_{difference} = |P_{compuer} - P_{sensor}|$$

$P_{difference}$が閾値P_{thresh}より大きい場合に、パッケージはタンパリングされたとみなされる。

【００１７】もう１つの実施例では、スマート・カードが、米国ニューヨーク州LathamのMarktech Optoelectronics社が製造する光検出器ＭＴＤ３０１０ＰＭなどの光センサを有する。このスマート・カードは、光にさらされないようにパッケージングされる。製品がタンパリングされる時には、光がこのセンサに達し、スマート・カードがこの変化を記録する。赤外放射や紫外放射などの可視スペクトルを超えた電磁放射を検出できる光電子センサを使用することができる。スペクトルのどの部分を使用する場合でも、前に圧力センサの場合で述べたように、ランダムなレベルを有する補助的な放射源を使用して、セキュリティを強化することができる。

【００１８】同様に、製品が出荷される温度をある範囲に維持しなければならない応用分野では、米国マサチューセッツ州NorwoodのAnalog Devices社が製造するＴＭＰ０３シリーズ・センサなどの温度センサを使用して、温度の変化を検出することができる。

【００１９】衝撃の検出が必要な自動車などの応用分野では、Analog Devices社のＡＤＸＬ０５またはLucas NovaSensor社のＮＡＣシリーズ加速度計などの加速度計を、センサ（またはセンサのうちの１つ）として使用することができる。

【００２０】スマート・タグ自動車センサの応用例の１つでは、スマート・カードが、ＡＤＸＬ０５の出力を記録し、タイム・スタンプを生成し、その結果を暗号化し、スマート・タグのメモリ１０３に記憶する。さらに、ＴＭＰ０３温度センサなどの他のセンサのログを記録し、記憶することもできる。自動車のスピードメータおよびオドメータの読みにタイム・スタンプを付け、暗号化し、メモリ１０３に記憶することもできる。自動車の位置は、その自動車がさらされた気象条件の種類を識別する際に重要であることがしばしばであり、出力がメモリ内に安全に記録されるＧＰＳシステムを追加することもできる。衝撃、温度、速度履歴、総マイル数履歴および地理的位置の時間履歴の組み合わせを使用して、自動車の状態を評価するために使用可能にすることができる安全な自動車の履歴を作成することができる。

【００２１】そのような履歴の例を、下に示す。

【表１】

自動車の履歴＝	総マイル数	８０，０００ｋｍ
	最大衝撃	１０ｇ
	最高温度	３２℃
	最低温度	１０℃
	最大速度	１３６ｋｍ／ｈ
	車両位置	フロリダ　走行距離の９０％
		その他　　走行距離の１０％

【００２２】製品によっては、センサ（またはセンサの組み合わせ）が、機械的特性、電磁的特性および熱的特性、より一般的には物理的特性または化学的特性もしくはその組み合わせを検出する。化学的特性を検出するセンサの参考資料は、ガードナ（J. Gardner）著、「An Introduction to Electronic Nose Technology」、Warwick刊、１９９６年に記載されている。センサ１０５で、ある固定された閾値を超える変化が検出された（または、センサによって捕捉されるデータが、計算されたランダム・シーケンスから十分に異なる）時に、それが、スマート・カード１０１内に不可逆的に記録される。事象にタイム・スタンプを付けることによって、装置の記録された履歴がもたらされる。安全なタイム・スタンプ付けは、たとえば、タンパ・プルーフ・パッケージ１０９の内部でスマート・カードにクロック・ユニットまたはタイミング・ユニットを接続することによって達成できる。

【００２３】図３からわかるように、たとえば、圧電気としてそのような物理的特性を使用する場合、Murata社のＰＤＧＳ－００ＬＡ－ＴＣ加速度計などのセンサ１０５は、センサの加速をもたらす外力入力に応答して、電圧として電子信号１１３を作る。電子信号１１３が、ある所定の閾値１１０を超える時には、比較器１１１がトリガされて、スマート・カードの電源を投入する論理レベル出力を作る。その結果、所定の閾値を超える衝撃が検出された時に、その衝撃が、スマート・カード１０１内に変化として不可逆的に記録される。同一の概念を、製品を含むパッケージへの侵入に対する保護のための追加手段としてランダム入力を受け入れるように適合させることができる。

【００２４】記録されるデータは、暗号化され、製品の物理的事象の履歴を提供する。（おそらくは公開）鍵を所有する人は、誰でもそのデータを取り出すことができ、そのデータは、正しいアルゴリズムによって処理されたならば、製品の状態の判定を可能にし、スマート・カードが取り付けられていると思われる製品にスマート・カードが取り付けられていることの認識を可能にする。このような分析には、製品がさらされた温度、製品が経験した衝撃、製品の電源が始めて投入された時刻などを含めることができるが、これらに制限されない。

【００２５】いくつかの場合には、必要であれば、スマート・カードが、やはり時刻を記録することによって、変更の履歴の記録も保持する。どの場合での、製品またはその環境の変化が、スマート・カードの状態の不可逆的な変更を引き起こす。これは、スマート・カードの内部メモリの消去またはある情報の書込によって実現することができる。

【００２６】製品が新しいか否かを判定したい人物は、だれでも、まずゼロ知識プロトコルを使用してスマート・カードを認証する。その人物は、次に、製品が開かれた、または、タンパリングされたかどうかに関する情報についてスマート・カードに問い合わせる。認証に成功し、スマート・カードに状態の変化が記録されていない場合には、その製品はタンパリングされていないと結論することができる。

【００２７】スマート・カードは、非接触式（認証または問合せを実行する時にカードとの物理的接触が不要であることを意味する）とすることができ、製品またはそのコンテナに組み込むことができる。この場合、認証と問合せは、なんらかのリモート手段を介して行われる。

このような技術は、現在使用可能である。たとえば、米国特許第５６８２１４３号明細書に開示されたＲＦＩＤである。それ以前の参考資料については、米国特許第４０６３２２９号明細書、米国特許第４２４２６６３号明細書および米国特許第４６４６０９０号明細書を参照されたい。

【００２８】いくつかの製品について、センサ１０５の出力は、オブジェクトまたはその環境の履歴の関数を決定するために数学的アルゴリズムを実行する処理ユニット１０４に送られる。たとえば、牛乳コンテナの温度と時刻の履歴を使用して、次式などのモデルに従って、牛乳が腐っている確率を判定することができる。

【数２】

$$P_{(sour)} = \int_{t_{manufacturedate}}^{t_{currentdate}} f(t,T(t))dt$$

ここで、Ｔは牛乳コンテナの温度、ｔは時刻、ｆは経験的に決定できる関数である。この処理は、暗号化することもしないこともできるメッセージをもたらすことができる。たとえば、このメッセージは、消費者が見ることのできるインジケータとすることができる。

【００２９】一部の製品（ワイン、食料、化学合成物、薬理学製品など）は、既知の理由なしに劣化する可能性があり、この場合、環境の制御だけを使用することはできず、なんらかのセンサで製品の本来の化学的または物理的特性を検出しなければならない。本発明の装置は、温度、湿度、圧力、光、振動、衝撃、電磁界、化学組成および製品を含むパッケージングの開封の記録に使用することができる。

【００３０】有効期限が過ぎたことを検出しなければならない場合には、スマート・カードに、製品の有効期限満了が発生した時にそれを記録するクロックまたはタイマを設けることができる。

【００３１】もう１つの実施例では、本発明の装置を、消費者電子製品の変更の検出および記録に使用することができる。さらに、前に述べた変化のほかに、製品の使用時間（通電時間）を記録することができる。

【００３２】スマート・カードは、非活動状態で作成することができる。スマート・カードを製品に取り付けた後に、スマート・カードにコマンドを送ることによってスマート・カードを活動化する。これは、非接触スマート・カードの場合にはリモートで行うことができる。活動化されたスマート・カードは、製品またはその環境の監視を開始する。セキュリティを高めるために、活動化されたスマート・カードは、破壊されるまで非活動化することができない。代替案では、非活動化が、スマート・カードが活動化の後に非活動化されたことを示すスマート・カードの不可逆変化を引き起こす。

【００３３】もう１つの好ましい実施例では、スマート・カードに、たとえばＲＦ（高周波）エネルギ源によって、外部から電力を供給することができる。スマート・カードは、製品がタンパリングされた時に変更される（たとえば、一部を破壊することができる）チップ上の形状を微細加工される。ユーザが、製品がタンパリングされたかどうかを判定する必要がある時には、外部電源を適用して、スマート・カードに電力を供給する。認証段階は前に説明したものと同一である。次に、微細加工された特徴を、スマート・カードまたはユーザのいずれかによって感知して、タンパリングが発生したかどうかを判定する。

【００３４】複数の応用分野と変更を有する好ましい実施例に関して本発明を説明してきたが、本発明を、請求項の趣旨および範囲の中で変更を加えて実施できることを、当業者は理解するであろう。

【００３５】まとめとして、本発明の構成に関して以下の事項を開示する。

【００３６】（１）オブジェクトまたは前記オブジェクトの環境の状態に関するデータを、複数のセンサのうちの少なくとも１つを用いて感知するステップと、前記センサからの信号をスマート・タグ内に組み込まれた記憶装置へ安全に送るステップと、後の取出のために前記記憶装置内で前記信号の暗号化を使用して安全に記録するステップとを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも１つに関する集積スマート・タグ内の情報を安全に記録し、記憶する方法。

（２）さらに、前記記憶装置内に記録された前記信号のそれぞれについて、前記記憶装置内で時刻を記録するステップを含む、上記（１）に記載の方法。

（３）前記センサが、温度、湿度、圧力、光、振動、衝撃、電磁界および化学組成を含むグループから選択された、前記オブジェクトの１つまたは複数の状態の変化を検出する、上記（１）に記載の方法。

（４）前記オブジェクトが、自動車であり、前記センサが、時刻、総マイル数、衝撃、温度、地理的位置、速度を含むグループのうちの少なくとも１つを検出し、前記記憶装置内で前記信号の暗号化を使用して安全に記録し、前記自動車の時間シーケンス履歴を作成する、上記（１）に記載の方法。

（５）前記オブジェクトが、薬理学製品、食品または化学製品を納めるパッケージング・コンテナであり、前記センサが、温度、湿度、圧力、光、振動、衝撃、電磁界、化学組成および前記パッケージング・コンテナの開封のグループのうちの少なくとも１つを検出する、上記（１）に記載の方法。

（６）前記オブジェクトが、電子消費者製品であり、前記センサが、前記消費者製品の電源投入時間の数を検出する、上記（１）に記載の方法。

（７）オブジェクトまたは前記オブジェクトの環境の状態に関するデータを、複数のセンサのうちの少なくとも

1つを用いて感知するステップと、前記データの複数の関数のうちの少なくとも1つを計算するために前記データを処理するステップと、前記データと前記関数の値との組み合わせを記憶装置に記憶するステップとを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも1つに関する集積スマート・タグ内の情報を記録し、記憶する方法。

（8）さらに、前記記憶装置での記憶の前に、前記データおよび前記関数の前記値のうちの少なくとも1つを暗号化するステップを含む、上記（7）に記載の集積スマート・タグに情報を記録し、記憶する方法。

（9）さらに、前記処理ステップからの結果を表示するステップを含む、上記（7）に記載の集積スマート・タグに情報を記録し、記憶する方法。

（10）記憶装置と、前記記憶装置に信号を安全に送るセンサと、後の取出のために前記記憶装置に安全に記録された前記信号からのデータを変更する暗号化モジュールとを含む、スマート・タグ・セキュリティ・システム。

（11）さらに、前記センサからの前記信号に作用する処理ユニットを含む、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（12）前記信号が前記記憶装置への記録に関する閾値を満たすかどうかを判定するために、前記処理ユニットが前記信号に作用する、上記（11）に記載のスマート・タグ・セキュリティ・システム。

（13）オブジェクトの状態を判定するために前記信号を処理するためのアルゴリズムを実行するために、前記処理ユニットが前記信号に作用する、上記（11）に記載のスマート・タグ・セキュリティ・システム。

（14）さらに、前記処理ユニットによって判定された結果を表示する表示装置を含む、上記（11）に記載のスマート・タグ・セキュリティ・システム。

（15）前記表示装置に、安全なアクセスが含まれる、上記（14）に記載のスマート・タグ・セキュリティ・システム。

（16）前記スマート・タグが、単一のシリコン基板に集積される、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（17）さらに、前記センサから記録される信号のそれぞれについて、記録されるタイム・スタンプを前記記憶装置に送るタイミング・ユニットを含む、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（18）前記センサが、前記センサの周囲の圧力の変化に応答して前記記憶装置に信号を送る圧力センサからなる、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（19）前記センサが、前記センサへの露光量が変化した時に前記記憶装置に信号を送る光センサからなる、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（20）前記センサが、破壊された場合に前記記憶装置に信号を送る電気接続からなる、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（21）さらに、前記セキュリティ・システムによって保護されるオブジェクトに固有の、前記記憶装置内で暗号化された識別コードを含む、上記（10）に記載のスマート・タグ・セキュリティ・システム。

（22）前記識別コードが、ゼロ知識プロトコルを使用して認証される、上記（21）に記載のスマート・タグ・セキュリティ・システム。

（23）オブジェクトまたは前記オブジェクトの環境の状態に関するデータを感知するためのセンサと、前記データの複数の関数のうちの1つを計算するためのプロセッサと、記憶装置に前記データと前記データの前記関数の値とを記憶するための記憶装置とを含む、時間にわたる前記オブジェクトに対する物理的、化学的および環境的影響のうちの少なくとも1つに関する集積スマート・タグ内の情報を記録し、記憶するためのスマート・タグ・セキュリティ・システム。

【図面の簡単な説明】

【図1】製品に取り付けられたスマート・タグを示す等角図である。

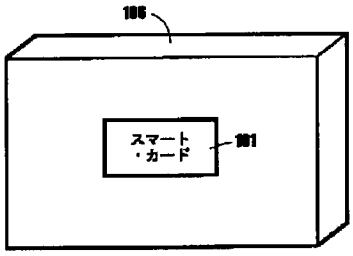
【図2】図1に示されたスマート・タグの詳細を示す平面図である。

【図3】センサから電気信号の作成までの経路を示す概略図である。

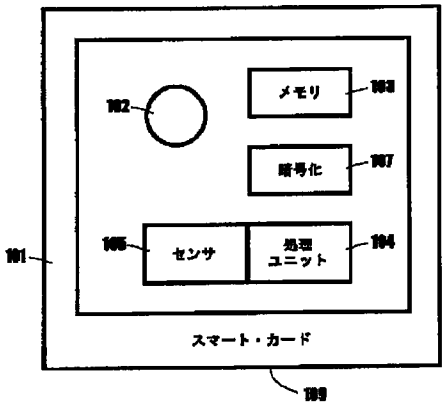
【符号の説明】

101　スマート・カード
102　電池
103　メモリ（または記憶装置）
104　処理ユニット
105　センサ
106　製品
107　暗号化モジュール
109　タンパ・プルーフ・パッケージ
110　閾値
111　比較器
113　電子信号

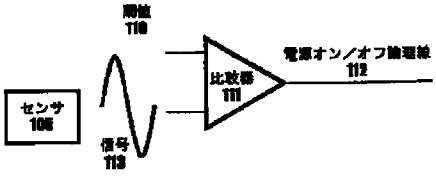
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者　クロード・エイ・グリーンガード
アメリカ合衆国10514　ニューヨーク州チャパクア　ジェフリー・レーン　40
(72)発明者　ウィリアム・アール・プーリーブランク
アメリカ合衆国10520　ニューヨーク州クロトン・オン・ハドソン　マクグァイア・レーン　2
(72)発明者　チャールズ・ピー・トレセ
アメリカ合衆国12570　ニューヨーク州ポークァグ　オーチャード・ドライブ　66
(72)発明者　チャイ・ダブリュー・ウー
アメリカ合衆国12570　ニューヨーク州ポークァグ　オーチャード・ドライブ　66